UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/675,399	09/29/2000	Carl Bilicska	Bilicska 3-2	9208

7590 09/09/2004

Troutman, Sanders, Mays & Valentine
Attn: John Curtin, Esq.
1660 International Dr.
Suite 600
McLean, VA 22102

EXAMINER	
MAHMOUDI, HASSAN	
ART UNIT	**PAPER NUMBER**
2175	

DATE MAILED: 09/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/675,399	**Applicant(s)** BILICSKA ET AL.	
	Examiner Tony Mahmoudi	**Art Unit** 2175	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 June 2004*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 June 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Remarks

1. In view of the Appeal Brief filed on 09-June-2004, PROSECUTION IS HEREBY REOPENED. New grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

2. Claims 1-14 are presently pending in the application.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that said subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-14 are rejected under 35 U.S.C. 102(b) as being unpatentable over Reed et al (U.S. Patent No. 5,862,325) in view of Ramasubramani et al (U.S. Patent No. 6,233,577B1.)

As to claim 1, Reed et al teaches an automated (see Abstract) authentication handling system (see column 26, lines 12-15) for use by clients (see column 26, lines 15-16) on a network (see Abstract, and see column 27, lines 62-64) comprising:

an authentication server (see column 97, line 60 through column 98, line 1) adapted to establish a two-way communication link (see column 76, lines 34-44, and see column 81, lines 59-67.)

Reed et al does not teach a two-way trusted communication link for access by an authenticated user to a list of application servers associated with a client identifier.

Ramasubramani et al teaches a centralized certificate management system (see Abstract), in which he teaches a two-way (see column 3, lines 20-22, and see column 5, lines 3-5) trusted communication link (see column 3, lines 48-52, and see column 6, lines 34-38) for access by an authenticated user to a list of application servers associated with a client identifier (see Abstract, where “list of application servers” is read on “plurality of secure servers”, see column 7, lines 41-45, where “authenticated user” is read on user with a created account, and “list of application servers” is read on “certain web servers”, also see column 8, lines 17-49, and see column 14, lines 6-25.)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Reed et al to include a two-way trusted communication link for access by an authenticated user to a list of application servers associated with a client identifier.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Reed et al by the teaching of Ramasubramani et al, because including a two-way trusted communication link for access by an authenticated user to a list of application servers associated with a client identifier, would enable the system to provide secure means for authenticated clients for accessing desired web sites hosted by various servers throughout a network. For example, the system can establish a two-way trusted (secured) communications link between authenticated users (shoppers) and various e-Commerce merchants, in which, the authenticity of the message and identity of the shopper (sender) would be validated by the merchant, as taught by Ramasubramani et al (see column 4, lines 18-28.)

As to claim 2, Reed et al as modified teaches wherein the authentication server (see Reed et al, column 97, line 60 through column 98, line 1) includes:

an identification engine configured to maintain collections of session assignments for accessing the application servers, each of the session assignment collections being associated with the client identifier (see Reed et al, column 26, lines 36-46, where "identification engine" is read on "system ID assignment function", "maintain collection of session assignments" is read on "control the access", also see Ramasubramani et al, column 8, lines 7-49.)

As to claim 3, Reed et al as modified teaches wherein the identification engine (see Reed et al, column 26, lines 36-46, where "identification engine" is read on "system ID assignment function") is adapted to receive client identifiers from the clients to establish authenticated users and responsive thereto to provide a user interface to access the application servers according to the associated session assignments (see Reed et al, column 26, lines 33-66, and see Ramasubramani et al, column 8, lines 17-22.)

As to claim 4, Reed et al as modified teaches wherein the authentication server (see Reed et al, column 97, line 60 through column 98, line 1) includes:

a communication initiator engine (see Reed et al, column 109, lines 19-28) configured to establish the trusted communication link between the authenticated users and an application server (see Reed et al, column 97, line 63 through column 98, line 1; column 100, lines 52-57; and see column 107, lines 44-51) on the list (see Ramasubramani et al, column 7, lines 41-45, where "list of application servers" is read on "certain web servers".)

As to claim 5, Reed et al as modified teaches wherein the authentication server (see Reed et al, column 97, line 60 through column 98, line 1) includes:

a communication initiator engine (see Reed et al, column 109, lines 19-28) configured to establish the trusted communication link (see Reed et al, column 100, lines 52-57, and see column 107, lines 44-51) defined to one of the session assignments between the authenticated users and the application server (see Reed et al, column 110, lines 35-44.)

As to claim 6, Reed et al as modified teaches wherein the session assignments include data fields (see Reed et al, column 67, line 64 through column 68, line 3) selected from the group consisting of session timeout and application access level (see Reed et al, column 70, line 63 through column 70, line 10.)

As to claim 7, Reed et al as modified teaches wherein the client identifier includes a user id and password (see Reed et al, column 72, lines 22-42, and see Ramasubramani et al, column 7, lines 10-16.)

As to claim 8, Reed et al as modified teaches wherein the authentication includes a processor under the control of software (see Reed et al, column 13, lines 7-12) to:

receive an authentication signal from the client (see Reed et al, column 28, lines 25-37);

provide an application access interface to the client in response to the authentication signal (see Reed et al, figures 22-24); and

establish the trusted communication link between the client and an application server selected from the application access interface (see Reed et al, column 100, lines 52-57, and see column 107, lines 44-51, and see Ramasubramani et al, column 3, lines 48-52, and see column 6, lines 34-38.)

As to claim 9, Reed et al teaches a method for automatically authenticating a client (see column 26, lines 12-15) for a plurality of application servers (see column 9, lines 50-65, and see column 25, lines 15-18) comprising the steps of:

providing an authentication server (see column 97, line 60 through column 98, line 1);

identifying clients for access to the application servers by the authentication server (see column 78, lines 25-32); and

Reed et al does not teach a two-way trusted communication link for access by an authenticated user to a list of application servers associated with a client identifier.

Ramasubramani et al teaches a centralized certificate management system (see Abstract), in which he teaches a two-way (see column 3, lines 20-22, and see column 5, lines 3-5) trusted communication link (see column 3, lines 48-52, and see column 6, lines 34-38) for access by an authenticated user to a list of application servers associated with a client identifier (see Abstract, where "list of application servers" is read on "plurality of secure servers", see column 7, lines 41-45, where "authenticated user" is read on user with a created account, and "list of application servers" is read on "certain web servers", also see column 8, lines 17-49, and see column 14, lines 6-25.)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Reed et al to include a two-way trusted communication link for access by an authenticated user to a list of application servers associated with a client identifier.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Reed et al by the teaching of Ramasubramani et al, because including a two-way trusted communication link for access by an authenticated user to a list of application servers associated with a client identifier, would enable the system to provide secure means for authenticated clients for accessing desired web sites hosted by various servers throughout a network. For example, the system can establish a two-way trusted (secured) communications link between authenticated users (shoppers) and various e-Commerce merchants, in which, the authenticity of the message and identity of the shopper (sender) would be validated by the merchant, as taught by Ramasubramani et al (see column 4, lines 18-28.)

As to claim 10, Reed et al as modified teaches wherein the identifying step includes:

providing session parameters for each of the identified clients for at least one of the application servers (see Reed et al, column 34, lines 18-47, and see Ramasubramani et al, column 14, lines 18-30, where "session parameters" is read on "device ID in the session request".)

As to claim 11, Reed et al as modified teaches wherein the identifying step includes:

providing a user interface to the identified clients for accessing the application servers (see Reed et al, column 68, lines 9-13, and see Ramasubramani et al, column 9, lines 29-32.)

As to claim 12, Reed et al as modified teaches wherein the establishing step includes:

using the session parameters (see Reed et al, column 34, lines 18-47, and see Ramasubramani et al, column 14, lines 18-30, where "session parameters" is read on "device ID in the session request") to establish the trusted communication link (see Reed et al, column 100, lines 52-57, and see column 107, lines 44-51, and see Ramasubramani et al, (see column 3, lines 48-52, and see column 6, lines 34-38.)

As to claim 13, Reed et al as modified teaches wherein the user interface includes a listing of application servers (see Ramasubramani et al, Abstract, where "listing of application servers" is read on "plurality of secure servers", and see column 7, lines 41-45, where "list of application servers" is read on "certain web servers") and the establishing step is initiated following a selection of an application server by a user from the user interface (see Reed et al, column 26, lines 47-64.)

As to claim 14, Reed et al as modified teaches the method further comprising a plurality of application servers connected to the network (see Ramasubramani et al, Abstract, where "listing of application servers" is read on "plurality of secure servers", and see column 7, lines 41-45, where "list of application servers" is read on "certain web servers"), each requiring authentication for access (see Reed et al, column 153, lines 20-23, and see Ramasubramani et al, column 7, lines 41-45.)

Response to Arguments

5. Applicant's arguments filed on 09-June-2004 with respect to the rejected claims in view of the cited references have been fully considered but they are moot in view of the new grounds of rejection.

Conclusion

6. Any inquiries concerning this communication or earlier communications from the examiner should be directed to Tony Mahmoudi whose telephone number is (703) 305-4887. The examiner can normally be reached on Mondays-Fridays from 08:00 am to 04:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici, can be reached at (703) 305-3830.

tm

August 23, 2004

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100